Resolución Directoral N°1981-2020-JUS/DGTAIPD-DPDP

Expediente N°
139-2019-JUS/DGTAIPD-PAS

Lima, 13 de noviembre de 2020

VISTOS:

El Informe Nº 113-2019-JUS/DGTAIPD-DFI de 30 de setiembre de 2019[1], emitido por la Dirección de Fiscalización e Instrucción de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la DFI), junto con los demás documentos que obran en el respectivo expediente; y,

CONSIDERANDO:

I. Antecedentes

1. El 05 de julio de 2018, personal de la DFI tomó conocimiento de la página web de Centro Medico Clínica San Judas Tadeo S.A., así como de la ubicación de su servidor de datos, por medio del aplicativo móvil "Whois, DNS, & Domain"[2].

2. Mediante Orden de Visita de Fiscalización Nº 81-2018-JUS/DGTAIPD-DFI[3], de 06 de julio de 2018, la DFI dispuso la realización de una visita de fiscalización a Centro Medico Clínica San Judas Tadeo S.A (en adelante, la administrada).

3. Mediante Acta de Fiscalización N° 01-2018[4], se deja constancia de los hallazgos encontrados durante la visita de supervisión realizada a las instalaciones de la administrada el 26 de julio de 2018, en su domicilio en calle Manuel Raygada N° 170, Urb. el Campillo, San Miguel, Lima.

4. Mediante Acta de Fiscalización N° 02-2018[5], se deja constancia de los hallazgos encontrados durante la visita de supervisión realizada a las instalaciones de la administrada el 26 de julio de 2018, en su domicilio en calle Laureano Martínez N°260, San Miguel, Lima.

[1] Folios 269 al 278
[2] Folios 2 al 6
[3] Folio 7
[4] Folio 8 a 12
[5] Folio 25 a 28

5. Mediante Acta de Fiscalización N° 03-2018[6], se deja constancia de los hallazgos encontrados durante la visita de supervisión realizada a las instalaciones de la administrada el 06 de agosto de 2018, en su domicilio en calle Laureano Martínez N°260, San Miguel, Lima.

6. Mediante Acta de Fiscalización N° 04-2018[7], se deja constancia de los hallazgos encontrados durante la visita de supervisión realizada a las instalaciones de la administrada el 06 de agosto de 2018, en su domicilio en calle Laureano Martínez N°115, San Miguel, Lima.

7. Con escrito ingresado el 07 de agosto de 29018 con registro Nº 51068[8], la administrada presentó documentación sobre medidas de seguridad

8. Mediante Acta de Fiscalización N° 05-2018[9], se deja constancia de los hallazgos encontrados durante la visita de supervisión realizada a las instalaciones de la administrada el 15 de agosto de 2018, en su domicilio en Av. Alameda Los Pinos N° 265 al 269, Chorrillos, Lima.

9. Con escrito ingresado el 13 de agosto de 2018 con registro Nº 52195[10], la administrada presento documentación solicitada en el Acta de Fiscalización N° 03-2018.

10. Con escrito ingresado el 13 de agosto de 2018 con registro Nº 52196[11], la administrada presentó documentación solicitada en el Acta de Fiscalización N° 01-2018, referida a la interacción lógica del banco de datos personales de pacientes.

11. Con escrito ingresado el 23 de agosto de 2018 con registro Nº 52810[12], la administrada presento el contrato de locación de instalación, operación, monitoreo y mantenimiento del sistema de alarmas a distancia.

12. Por medio del Informe Técnico N° 205-2018-DFI-ETG[13], el Analista de Fiscalización en Seguridad de la Información de la DFI señaló que la administrada no cumple con las medidas de seguridad de información adecuadas, de acuerdo con lo previsto en la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, LPDP) y su reglamento, aprobado por Decreto Supremo N° 003-2013-JUS (en adelante, Reglamento de la LPDP).

13. Mediante el correo electrónico de 09 de noviembre de 2018[14], el personal a cargo del Registro Nacional de Protección de Datos Personales (en adelante, RNPDP) informó que la administrada contaba con bancos de datos personales denominados “Paciente”, “Videovigilancia”, “Proveedores” y “Trabajadores” inscritos, así como no

[6] Folio 33 a 37
[7] Folio 52 a 56
[8] Folios 69 al 81
[9] Folio 87 a 91
[10] Folios 93 al 123
[11] Folios 125 al 128
[12] Folios 129 al 135
[13] Folios 136 al 141
[14] Folio 142

tenía registrada ninguna comunicación de flujo transfronterizo, ni solicitud pendiente de atención .

14. Por medio del Informe de Fiscalización Nº 176-2018-JUS/DGTAIPD-DFI-PCFC del 07 de diciembre de 2018[15], se puso en conocimiento de la DFI los resultados de la fiscalización adjuntando las actas de fiscalización, así como los demás anexos y documentos que conforman el respectivo expediente administrativo, dicho informe fue notificado a la administrada el 26 de diciembre de 2018, a través del Oficio Nº 865-2018-JUS/DGTAIPD-DFI[16] .

15. A través de la comunicación ingresada con registro N° 4064-2019[17] de 18 de enero de 2019, la administrada presento escrito señalando haber tomado nota de las conclusiones expresadas en el informe de fiscalización.

16. Por medio del escrito ingresado con Registro N° 40222-2019[18] de fecha 06 de junio de 2019, la administrada presenta acciones realizadas en base al Informe de Fiscalización Nº 176-2018-JUS/DGTAIPD-DFI-PCFC.

17. Por medio del Informe Técnico N°143-2018-DFI-ETG[19], el Analista de Fiscalización en Seguridad de la Información de la DFI señaló que la administrada no cumple con las medidas de seguridad de información.

18. Mediante la Resolución Directoral Nº 149-2019-JUS/DGTAIPD-DFI del 14 de agosto de 2019[20], la DFI resolvió iniciar procedimiento administrativo sancionador a la administrada, por la presunta comisión de las siguientes infracciones:

    i. Realizar tratamiento de datos personales a través de: "Registro de pacientes del sistema SJT", mediante los formularios físicos denominados "Tapa principal de historias clínicas", hoja de atención de emergencias", "Declaración de alergias a medicamentos y/o alimentos" y "Historias clínicas ambulatorias", y mediante las cámaras de videovigilancia; sin informar a los titulares de datos personales lo requerido en el artículo 18° de la LPDP; lo que configuraría una infracción grave tipificada en el literal a, numeral 2 del artículo 132° del Reglamento de la LPDP: *"No atender impedir u obstaculizar el ejercicio de los derechos del titular de datos personales reconocidos en el título III de la Ley N° 29733 y su Reglamento".*

    ii. No haber implementado las medidas de seguridad para el tratamiento de datos personales al:

        a. No documentar los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados. Obligación establecida en el numeral 1 del artículo 39° del Reglamento de la LPDP.

[15] Folios 145 al 153
[16] Folios 154 al 155
[17] Folios 156 al
[18] Folios 158 al 177
[19] Folio 179
[20] Folios 186 al 198

b. No generar ni mantener registros de interacción lógica respecto al banco de datos personales en soporte automatizado de pacientes. Obligación establecida en el numeral 2 del artículo 39° del Reglamento de la LPDP.

.

Lo que configuraría la infracción leve tipificada en el literal a), numeral 1, del artículo 132° del Reglamento de la LPDP: *"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normatividad sobre la materia."*

19. Dicha Resolución Directoral fue notificada a la administrada el 27 de agosto de 2019, a través del Oficio Nº 710-2019-JUS/DGTAIPD-DFI[21].

20. Mediante escrito con registro N° 67452 de fecha 23 de setiembre de 2019[22], la administrada presento descargos alegando lo siguiente:

- Respecto de la imputación referida a no informar las disposiciones establecidas en el artículo 18° de la LPPD, la administrada alega haber implementado dentro del ámbito a la LPDP la política de privacidad la cual fue colocada en distintos ambientes con la finalidad de cumplir con informar a los titulares de datos personales.
- Asimismo, señala que la información recopilada resulta necesario y pertinente para las finalidades determinadas, toda vez que es información que se consigna de manera obligatoria en las historias clínicas.
- Sobre no documentar los procedimientos de gestión de accesos de privilegios y verificación periódica de privilegios asignados, la administrada precisa que los responsables que autorizan los usuarios de ingreso al sistema del banco de datos automatizado de pacientes son gerencia general, gerencia de operaciones y jefatura de sistemas.
- De no generar ni mantener registros de interacción lógica respecto al banco de datos personales en soporte automatizado de pacientes, la administrada señala que con fecha 13 de agosto de 2019 remitió los registro de interacción lógica del banco de datos personales de pacientes.

21. Al respecto, mediante Informe Técnico Nº 189-2019-DFI-ETG[23] de fecha 25 de setiembre de 2019, emitido por el Analista de Fiscalización en Seguridad de la Información, recoge lo siguiente:

> *"(…)*
> ***III. Conclusiones***
> *1. CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A., no documenta los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados, incumpliendo con el numeral 1 del artículo 39° del Reglamento de la LPDP*

[21] Folio 199 al 201
[22] Folios 202 a 262
[23] Folio 264

> *2. CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A., no genera ni mantiene registros de interacción lógica respecto al banco de datos personales en soporte automatizado de pacientes, incumpliendo con el numeral 2 del artículo 39° del Reglamento de la LPDP.*
>
> *(…)"*

22. Mediante Resolución Directoral N° 176-2019-JUS/DGTAIPD-DFI[24] de 30 setiembre de 2019, la DFI dio por concluidas las actuaciones instructivas correspondientes al procedimiento sancionador. Dicha resolución fue notificada a la administrada el 15 de octubre de 2019, a través del Oficio N° 804-2019-JUS/DGTAIPD-DFI[25].

23. A través del Informe N° 113-2019-JUS/DGTAIPD-DFI[26], la DFI remitió a la DPDP el expediente del presente caso, recomendando lo siguiente:

i. Imponer una multa ascendente a siete unidades impositivas tributarias (7 UIT) a Centro Medico Clínica San Judas Tadeo S.A., por el cargo acotado en el Hecho N° 01; por la infracción grave prevista en el literal a) del numeral 2 del artículo 132 del Reglamento de la LPDP: *"No atender, impedir u obstaculizar el ejercicio de los derechos de los derechos del titular de datos personales reconocidos en el título III de la Ley N° 29733 y su reglamento".*

ii. Imponer una multa ascendente a dos coma cinco unidades impositivas tributarias (2,5 UIT), a Centro Medico Clínica San Judas Tadeo S.A por el cargo acotado en el Hecho N° 02; por la infracción leve prevista en el literal a) del numeral 1 del artículo 132 del Reglamento de la LPDP: *"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normatividad sobre la materia".*

24. Mediante el escrito ingresado con la Hoja de Trámite N° 74063-2019 de 18 de octubre de 2019[27], la administrada presentó descargos argumentando lo siguiente:

- Que los fiscalizadores no han tomado consideración de los carteles que se encuentran distribuidos en nuestras instalaciones, por lo que no se puede suponer que los titulares de datos no tengan conocimiento de los tratamientos de sus datos personales, toda vez que en dichos carteles de señala lo siguiente:

> *"Centro Médico Clínica San Judas Tadeo S.A., con domicilio en Calle Manuel Raygada N° 170, Urb. El Campillo, San Miguel, Lima-Perú, es responsable de recabar sus datos personales, del uso que se le dé a los mismos y de su protección. Su información personal será utilizada para proveer los servicios y productos que ha solicitado, informarle sobre cambios en los mismos y evaluar la calidad del servicio. La base de datos se almacena en la dirección de la Clínica Santa Isabel en forma*

[24] Folio 265 al 267
[25] Folio 268
[26] 269 a 278
[27] Folios 279 al 333

mixta, (digital y física, para el caso de las Historias Clínicas). Siendo que, dependiente de la recopilación de los datos, estos estarán registrados en las Bases de Datos: PACIENTES, VIDEO VIGILANCIA.

La conservación y transferencia de sus datos personales se aplican de acuerdo a la normatividad vigente como la Ley General de Salud N° 26842, la Ley de Protección de Datos Personales y su Reglamento. Los datos serán registrados según fueron inscritas las Bases de Datos, siendo que, para el caso de Video Vigilancia, estos serán almacenados durante 30 días calendario; y, para los datos recopilados de Pacientes, estos serán almacenados según lo señala la normativa vigente.

Cabe señalar que, la negativa a proporcionar sus datos personales y sensibles, nos imposibilita brindarle la atención médica correspondiente y por la cual recurre a nuestra Institución. En ese sentido, se entenderá que ha otorgado su consentimiento si usted no manifiesta su oposición explicita para el tratamiento de datos sus personales.

Asimismo, en aras de cumplir con lo establecido en normativa vigente, usted podrá hacer valer sus derechos ARCO (Derechos de Acceso, Rectificación, Cancelación y Oposición) a través de nuestra Gerencia de Sistemas, mediante comunicación remitida en la siguiente dirección: Calle Manuel Raygada N° 170, Urb. El Campillo, San Miguel, Lima- Perú."

- Conforme, lo antes descrito, la administrada precisa haber cumplido con informar a los usuarios lo correspondiente al manejo de sus datos personales señalando que los fiscalizadores precisaron que la información debe ser puesta en conocimiento de los titulares de datos personales de manera escrita en hoja adicional, la cual debe contar con cargo de recepción, en ese sentido la administrada alega que no está estipulado en la norma advirtiendo que generaría un perjuicio económico, toda vez que tendrían que generar documentos adicionales a los que usualmente se entregan.

- Por otro lado, la administrada precisa que cuenta con carteles, a través de los cuales se da aviso a los titulares de datos personales que están siendo filmados y en cuanto al tratamiento efectuado a los datos personales recopilados por las cámaras se encuentra indicado en las políticas de privacidad que se encuentran distribuidos en las instalaciones.

- Sobre la indicado por DFI en el informe final referido a que las políticas de privacidad no se menciona el tiempo de conservación, precisando que lo que se indicó es ambiguo "(…) *estos serán almacenados según normativa vigente",* la administrada señala que al mencionar el tiempo se ciñe a la normativa NTS N° 139-MINSA/2018/DGAIN — "Norma Técnica de Salud para la Gestión de Historia Clínica", la cual dispone que el plazo máximo de conservar la información es de 20 años, en caso de contabilizar el tiempo que debe ser conservada en archivo activo y pasivo existe la excepción de conserva dicha información por 40 años.

- Conforme a los argumentos expuestos la administrada señala haber cumplido con informar lo dispuesto en el artículo 18° de la LPDP.

- Respecto a la imputación sobre las medidas de seguridad, la administrada manifestó que la documentación ha sido adjuntado y obra en el expediente administrativo sancionador en los que se especifican claramente los procedimientos que establece la normativa de la materia.

- Para finalizar, la administrada alega haberse vulnerado los principios de la potestad sancionadora.

25. Mediante Oficio N° 2968-2019-JUS/DGTAIPD-PAS[28] de fecha 15 de noviembre de 2019, la DPDP programó informe oral para el día 9 de diciembre de 2019 a horas 10:30 a.m. conforme al Registro de Asistencia[29] dicho informe se llevó acabo en la fecha y hora señalada.

26. Con Resolución Directoral Nº 1111-2020-JUS/DGTAIPD-DPDP[30] de fecha 17 de julio de 2020, la DPDP resolvió ampliar por tres (3) meses el plazo de caducidad contados desde 17 de agosto de 2020, dicha resolución fue notificada el 22 de agosto de 2020, a través del Oficio Nº 973-2020-JUS/DGTAIPD-DPDP[31].

27. Mediante Oficio Nº 1231-2020-JUS/DGTAIPD-DPDP[32] de fecha 3 de setiembre de 2020, la DPDP solicitó a la DFI informe técnico sobre las medidas de seguridad implementadas por la administrada.

28. En ese sentido, con Oficio Nº1176-2020-JUS/DGTAIPD-DFI[33] de fecha 11 de octubre de 2020, la DFI adjuntó el Informe Técnico Nº 376-2020-DFI-ETG[34]

29. Mediante escrito de fecha 05 de agosto de 2020[35], la administrada presentó la información solicitada mediante Resolución Directoral Nº 1111-2020-JUS/DGTAIPD-DPDP, en los que señala tener en cuenta lo dispuesto en los principios de la potestad sancionadora a fin de resolver conforme a derecho.

II. Competencia

30. De conformidad con el artículo 74 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo N° 013-2017-JUS, la DPDP es la unidad orgánica competente para resolver en primera instancia, los procedimientos administrativos sancionadores iniciados por la DFI.

31. En tal sentido, la autoridad que debe conocer el presente procedimiento sancionador, a fin de emitir resolución en primera instancia, es la directora de Protección de Datos Personales.

[28] Folio 334
[29] Folio 335
[30] Folios 336 al 338
[31] Folios 339 al 340
[32] Folio 351
[33] Folio 348
[34] Folio 349 al 351
[35] Folios 341 al 345

III. Normas concernientes a la responsabilidad de la administrada

32. Acerca de la responsabilidad de la administrada, se deberá tener en cuenta que el literal f) del numeral 1 del artículo 257 de la LPAG, establece como una causal eximente de la responsabilidad por infracciones, la subsanación voluntaria del hecho imputado como infractor, si es realizada de forma previa a la notificación de imputación de cargos[36].

33. Asimismo, se debe atender a lo dispuesto en el artículo 126 del Reglamento de la LPDP, que considera como atenuantes la colaboración con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones conjuntamente con la adopción de medidas de enmienda; dichas atenuantes, de acuerdo con la oportunidad del reconocimiento y las fórmulas de enmienda, pueden permitir la reducción motivada de la sanción por debajo del rango previsto en la LPDP[37].

34. Dicho artículo debe leerse conjuntamente con lo previsto en el numeral 2 del artículo 257 de la LPAG38, que establece como condición atenuante el reconocimiento de la responsabilidad por parte del infractor de forma expresa y por escrito, debiendo reducir la multa a imponérsele hasta no menos de la mitad del monto de su importe; y, por otro lado, las que se contemplen como atenuantes en las normas especiales.

IV Primera cuestión previa: sobre la legalidad de la norma bajo la cual se pretende sancionar a la administrada

35. La administrada, en su escrito presentado el 18 de octubre de 2019 (folio 2280 a 333) y escrito de 05 de agosto de 2020 (folios 341 al 345) señala que en el presente procedimiento se ha vulnerado el principio de legalidad en sentido estricto, toda vez que una persona natural o jurídica no puede ser condenada o sancionada por un

[36] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS**
"**Artículo 257.- Eximentes y atenuantes de responsabilidad por infracciones**
1.- Constituyen condiciones eximentes de la responsabilidad por infracciones las siguientes:
(…)
f) La subsanación voluntaria por parte del posible sancionado del acto u omisión imputado como constitutivo de infracción administrativa, con anterioridad a la notificación de la imputación de cargos a que se refiere el inciso 3) del artículo 255."

[37] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 003-2013-JUS**
"**Artículo 126.- Atenuantes.**
La colaboración con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones acompañado de acciones de enmienda se considerarán atenuantes. Atendiendo a la oportunidad del reconocimiento y a las fórmulas de enmienda, la atenuación permitirá incluso la reducción motivada de la sanción por debajo del rango previsto en la Ley"

[38] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS**
"**Artículo 257.- Eximentes y atenuantes de responsabilidad por infracciones**
(…)
2.- Constituyen condiciones atenuantes de la responsabilidad por infracciones las siguientes:
a) Si iniciado un procedimiento administrativo sancionador el infractor reconoce su responsabilidad de forma expresa y por escrito.
En los casos en que la sanción aplicable sea una multa esta se reduce hasta un monto no menor de la mitad de su importe.
b) Otros que se establezcan por norma especial."

delito o infracción no prevista expresamente en una norma con rango de ley. Por otro lado, se vulnera el subprincipio de tipicidad o taxatividad cuando, pese a que la infracción o delito está prevista en una norma con rango de ley, la descripción de la conducta punible no cumple con estándares mínimos de precisión.

36. Al respecto, corresponde precisar las particularidades del principio de tipicidad en relación a los alcances del principio de legalidad. El principio de legalidad, refiere al instrumento normativo en el que debe preverse la potestad sancionadora, así como las infracciones y sanciones correspondientes. De otro lado, el principio de tipicidad alude al grado de predeterminación normativa de las conductas típicas proscribiendo supuestos de interpretación extensiva o analógica, es decir, corresponde sancionar un hecho cuando este se encuentre definido y tenga claramente definida su penalidad. Asimismo, el principio de tipicidad no se encuentra sujeto a una reserva de ley absoluta, pues en determinadas situaciones podría ser complementado a través de los reglamentos respectivos.

37. No obstante, la DPDP considera que, habiéndose determinado que la LPDP regula las infracciones y las sanciones respectivas, en sus artículos 38[39] y 39[40], corresponde indicar lo señalado en la Sentencia del Tribunal Constitucional de 10 de noviembre de 2015 (Pleno Jurisdiccional) recaída en los Expedientes N° 0014-2014-P1/TC, 0016-2014-PI/TC, 0019-2014-P1/TC y 0007-2015-PI/TC que indica los siguientes aspectos referidos al principio de legalidad y reserva de ley relativa:

> *(…)*
> *180. En esta materia aplica entonces aquella reserva de ley relativa. Por ende, no resulta inconstitucional que se derive al reglamento la tipificación de las infracciones, en tanto se ha fijado en la ley las conductas sancionables y la escala y los tipos de sanción.*
> *181. Por último, cabe añadir que si se regula una actividad con miras a garantizar la calidad del servicio público, resulta necesario dotar al organismo supervisor de las herramientas necesarias para corregir las infracciones que se adviertan en su ámbito específico.*

[39] **Artículo 38.- Tipificación de infracciones**
Las infracciones se clasifican en leves, graves y muy graves, las cuales son tipificadas vía reglamentaria, de acuerdo a lo establecido en el numeral 4) del artículo 230 de la Ley Nº 27444, Ley del Procedimiento Administrativo General, mediante Decreto Supremo con el voto aprobatorio del Consejo de Ministros. (…).

[40] **Artículo 39. Sanciones administrativas**
En caso de violación de las normas de esta Ley o de su reglamento, la Autoridad Nacional de Protección de Datos Personales puede aplicar las siguientes multas:
1. Las infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).
2. Las infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT).
3. Las infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT).
(…)
La Autoridad Nacional de Protección de Datos Personales determina la infracción cometida y el monto de la multa imponible mediante resolución debidamente motivada. Para la graduación del monto de las multas, se toman en cuenta los criterios establecidos en el artículo 230, numeral 3), de la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces. (…).

> *182. De otro lado, y como es obvio, las resoluciones de sanción deberán estar debidamente motivadas, y la sanción que se imponga debe resultar proporcional a la naturaleza y gravedad de la infracción en que haya incurrido.*
> *(…)*

38. Por el principio de tipicidad, las disposiciones reglamentarias de desarrollo solamente pueden "especificar o graduar" aquellas normas dirigidas a identificar las conductas (infracciones) o determinar sanciones, sin constituir nuevas conductas sancionables a las previstas legalmente, salvo los casos en que una ley o decreto legislativo permita tipificar infracciones por norma reglamentaria como se advierte de la normativa que regula la protección de datos personales, específicamente el artículo 38 de la LPDP.

V. Segunda cuestión previa: Sobre la vinculación entre el Informe de Instrucción y el pronunciamiento de esta dirección

39. El artículo 254 de la LPAG establece como carácter fundamental del procedimiento administrativo sancionador, la separación entre la autoridad instructora y la autoridad sancionadora o resolutora:

> **"Artículo 254.- Caracteres del procedimiento sancionador**
> 254.1 Para el ejercicio de la potestad sancionadora se requiere obligatoriamente haber seguido el procedimiento legal o reglamentariamente establecido caracterizado por:
> 1. Diferenciar en su estructura entre la autoridad que conduce la fase instructora y la que decide la aplicación de la sanción.
> (…)"

40. Por su parte, el artículo 255 de dicha ley, establece lo siguiente:

> **"Artículo 255.- Procedimiento sancionador**
> Las entidades en el ejercicio de su potestad sancionadora se ciñen a las siguientes disposiciones:
> (…)
> 5. Concluida, de ser el caso, la recolección de pruebas, la autoridad instructora del procedimiento concluye determinando la existencia de una infracción y, por ende, la imposición de una sanción; o la no existencia de infracción. La autoridad instructora formula un informe final de instrucción en el que se determina, de manera motivada, las conductas que se consideren probadas constitutivas de infracción, la norma que prevé la imposición de sanción; y, la sanción propuesta o la declaración de no existencia de infracción, según corresponda.
>
> Recibido el informe final, el órgano competente para decidir la aplicación de la sanción puede disponer la realización de actuaciones complementarias, siempre que las considere indispensables para resolver el procedimiento. El informe final de instrucción debe ser notificado al administrado para que formule sus descargos en un plazo no menor de cinco (5) días hábiles.

41. De los artículos transcritos, se desprende que la separación de las dos autoridades, así como la previsión de ejercicio de actuaciones por parte de la autoridad sancionadora o resolutora implican la autonomía de criterios de ambas, siendo que la segunda de las mencionadas puede hacer suyos todos los argumentos, conclusiones y recomendaciones expuestos por la autoridad instructora en su informe final de instrucción, así como, en sentido distinto, puede efectuar una distinta evaluación de los hechos comprobados, cuestionarlos o inclusive calificar situaciones que si bien fueron tomadas en cuenta al momento de efectuar la imputación, no fueron correctamente evaluadas al finalizar la instrucción.

42. Por tal motivo, la resolución que emita una autoridad sancionadora o resolutora, puede apartarse de las recomendaciones del informe final de instrucción, haciendo una evaluación diferente, considerando la naturaleza no vinculante de aquel informe, y sin que ello implique una vulneración de la predictibilidad o de la expectativa legítima del administrado, la cual no encuentra asidero en la normativa referida al procedimiento administrativo, en la que no se establece ningún elemento que establezca la obligatoria observancia del mismo.

VI. Cuestiones en discusión

43. Corresponde a esta dirección determinar si se han cometido infracciones a la LPDP y su Reglamento, para lo cual se deberá analizar:

    43.1 Si la administrada es responsable de los siguientes hechos infractores:

    - Realizar tratamiento de datos personales a través de: “Registro de pacientes del sistema SJT”, mediante los formularios físicos denominados “Tapa principal de historias clínicas”, hoja de atención de emergencias”, “Declaración de alergias a medicamentos y/o alimentos” y “Historias clínicas ambulatorias”, y mediante las cámaras de videovigilancia; sin informar a los titulares de datos personales lo requerido en el artículo 18° de la LPDP.

    - No haber implementado las medidas de seguridad para el tratamiento de datos personales al: (i) No documentar los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados. Obligación establecida en el numeral 1 del artículo 39° del Reglamento de la LPDP. (i) No generar ni mantener registros de interacción lógica respecto al banco de datos personales en soporte automatizado de pacientes. Obligación establecida en el numeral 2 del artículo 39° del Reglamento de la LPDP.

44. En el supuesto de no ser responsable en cada caso, si debe aplicarse la exención de responsabilidad por la subsanación de la infracción, prevista en el literal f) del numeral 1 del artículo 257 de la LPAG, o las atenuantes, de acuerdo con lo dispuesto en el artículo 126 del reglamento de la LPDP.

45. Determinar en cada caso, la multa que corresponde imponer, tomando en consideración los criterios de graduación contemplados en el numeral 3) del artículo 248° de la LPAG.

Sobre el deber de información establecido en el artículo 18° de la LPDP

46. El artículo 18° de la LPDP establece el derecho de los titulares de los datos personales deben ser informados sobre el tratamiento que se realizará con aquellos, disponiendo los siguiente:

> *"**Artículo 18. Derecho de información del titular de datos personales***
> *El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del o de los encargados del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello.*
>
> *Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables."*

47. Así, de la normas acotadas se desprende que los titulares de los datos personales tienen derecho a ser informados sobre el tratamiento que se realizará a su información personal, el fin de su recopilación y almacenamiento de los datos personales, si existe un banco de datos que conservará la información (sea nacional o internacional), el tiempo de la conservación, qué personas se encargarán de administrar la información y los terceros destinatarios de aquella si los hubiera, nacionales o internacionales.

48. En este caso, en el Acta de Fiscalización N° 01- 2018[41] se dejó constancia de la visita de supervisión realizada a la administrada el 26 de julio de 2018, precisando que:

> *"(…) Se fiscalizó el banco de datos personales de Pacientes, el cual realiza tratamiento en soporte automatizado y no automatizado (…) posee el sistema cliente servidor denominado SJT, a través del cual realizan tratamiento de datos personales en soporte automatizado. (…)."*

49. En el Acta de Fiscalización N° 03- 2018[42] se dejó constancia de la visita de supervisión realizada a la administrada el 06 de agosto de 2018, precisando que:

[41] Folio 08 al 12
[42] Folio 08 al 12

"(…) 3.- Se verificó que cuenta con un ambiente denominado "Sala de Videovigilancia", la cual se encuentra a cargo de la jefa de mantenimiento (…)."

50. En el Acta de Fiscalización N° 04- 2018[43] se dejó constancia de la visita de supervisión realizada a la administrada el 06 de agosto de 2018, precisando que:

"(…) Se verificó que las Historias Clínicas están ordenadas por número en forma ascendente (…)."

51. Luego, con el Informe de Fiscalización N° 176-2018-JUS/DGTAIPD-DFI-PCFC[44] de 07 de diciembre de 2019 que recoge las conclusiones sobre el procedimiento de fiscalización, se indica lo siguiente:

"(…)
VII. CONCLUSIONES
(…)
Segunda. *-* ***CENTRO MEDICO CLINICA SAN JUDAS TEDEO S.A.*** estaría realizando tratamiento de datos personales, sin informar a los titulares de los datos lo requerido por el artículo 18° de la LPDP, lo que vulneraría su derecho de información sobre las condiciones del tratamiento de sus datos personales. Hecho que constituiría una presunta infracción, según lo regulado en el literal a, numeral 2, artículo 132° del RLPDP: *"No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo a lo establecido en el Título III de la Ley N° 29733 y su Reglamento",* dicha infracción es **grave** conforme al citado artículo.
(…)"

52. De los documentos citados y de las impresiones web obrantes en el expediente, se colige que al momento de la fiscalización la administrada realizaba tratamiento de datos personales, sin informar lo requerido en el artículo 18° de la LPDP.

53. En el presente caso, se imputa como hechos infractores a través de la Resolución Directoral Nº 149-2019-JUS/DGTAIPD-DFI, efectuar el tratamiento utilizando los siguientes medios:

- Sistema cliente/servidor denominado "Registro de pacientes del sistema SJT"
- Formularios físicos denominados "Tapa principal de historias clínicas", hoja de atención de emergencias", "Declaración de alergias a medicamentos y/o alimentos" y "Historias clínicas ambulatorias"
- Cámaras de Videovigilancia.

54. En primer lugar, se tiene que la administrada realiza tratamiento de datos personales a través del sistema cliente/servidor denominado "Registro de pacientes del sistema SJT".

[43] Folio 33 al 37
[44] Folio 52 al 56

55. Al respecto, con fecha 23 de setiembre de 2019, la administrada presentó descargos, no obstante, de la lectura a dicho escrito se evidencia que la administrada no presenta argumentos específicos sobre el tratamiento de datos personales mediante el sistema cliente servidor SJT.

56. Al respecto, la DFI mediante Informe N° 113-2019-JUS/DGTAIPD-DFI de fecha 30 de setiembre de 2019, indica que no figura medio probatorio alguno, a través del cual la administrada informe a los titulares de datos personales lo dispuesto en el artículo 18° de la LPDP.

57. Posteriormente, la administrada con fecha 18 de octubre de 2019 presentó descargos, no obstante, no presenta argumentos específicos sobre el tratamiento realizado por el sistema denominado "Registro de pacientes del sistema SJT"

58. Por lo que, de lo consignado en el Acta de Fiscalización N° 01-2018, captura de pantalla obrante en folio 24 y demás documentos contenidos en el presente expediente administrativo, la DPDP debe advertir que la administrada si bien realiza tratamiento de datos a través del mencionado sistema, no se ha probado de qué forma se ingresa la información al sistema, por lo tanto no se ha acreditado si es información que se toma de los formularios llenados por el paciente, o si se recopilan los datos de forma directa del paciente, por lo que no existe certeza sobre el incumplimiento respecto a los señalado en el artículo 18° de la LPDP, sobre dicho extremo de la imputación.

59. Por lo tanto, esta dirección considera declarar infundado el extremo de la imputación referida a la obligación de informar lo dispuesto en el artículo 18º de la LPDP lo relacionado al sistema cliente/servidor denominado "Registro de pacientes en el Sistema SJT".

60. En segundo lugar, se tiene que la administrada realiza tratamiento de datos personales a través de formularios físicos denominados Tapa principal de historias clínicas", hoja de atención de emergencias", "Declaración de alergias a medicamentos y/o alimentos" y "Historias clínicas ambulatorias"

61. Al respecto, con fecha 23 de setiembre de 2019[45] la administrada presentó descargos alegando lo siguiente:

    - Que los datos personales recopilados en los formularios "Tapa principal de la Historia Clínica", "Hoja de atención de emergencia", "Declaración de alergias, etc., son en estricto cumplimiento de la Norma Técnica de Salud.

    - No obstante, la administrada alega que dentro del ámbito de la LPDP implemento el documento Política de Privacidad, el cual fue colocado en diversos ambientes, por lo que como medio de prueba adjuntan fotografías.

[45] Folios 202 al 262

- La administrada adjunta copia del documento denominado “Política de Privacidad”, en mismo que se ubica en folios 246.

62. Al respecto, la DFI mediante Informe N° 113-2019-JUS/DGTAIPD-DFI indica lo siguiente *“(…) c) Respecto al aviso de "Política de privacidad" (f. 246), es preciso señalar que la información debe ser proporcionada al titular de los datos en el momento en que éstos se solicitan, previamente a que sean recopilados, por tanto, en el caso de los datos personales solicitados mediante soporte no automatizado, la manera idónea de entregarla es en el documento a través del cual se solicitan y no publicándola en el establecimiento, debido a que esta modalidad no demuestra que efectivamente el titular del dato haya tomado conocimiento de las condiciones del tratamiento de sus datos personales. Pudiendo los carteles usarse en adición a la información entregada directamente al interesado, o en todo caso dejar constancia en el documento que se afilia, que se ha informado al interesado que las condiciones del tratamiento de sus datos se encuentran en avisos colocados (…).*

63. En tal sentido, es importante tener presente que el derecho de información es uno de los principales derechos que tiene toda persona natural cuando se realiza un tratamiento de los datos que la identifican como tal o la hacen identificable, en tanto le permite como mínimo conocer la finalidad para la cual se están recopilando sus datos, así como a quién o a quiénes podrán ser transferidos y la manera de cómo y frente a quién podrá ejercer sus derechos ARCO (acceso, rectificación, cancelación y oposición). Es en respuesta al reconocimiento de dicho derecho que toda información sobre las condiciones del tratamiento de los datos personales debe ser fácilmente identificable y accesible, de forma previa a su recopilación, por parte de los titulares de los mismos. Para ello, y en cumplimiento del deber de informar contenido en el artículo 18° de la LPDP, todo titular de bancos de datos personales o responsable del tratamiento de datos personales tiene la obligación de poner a disposición de los titulares de los mismos toda información relevante vinculada a su tratamiento.

64. En ese sentido, la DPDP procedió al análisis del documento denominado “Política de Privacidad”, observando que la administrada no cumple con indicar lo siguiente: (i) la transferencia de los datos personales indicando a nivel nacional las empresas destinatarias de los datos personales, la finalidad de la transferencia, y en caso la transferencia sea internacional debe indicar denominación de la empresa, país y finalidad de dicha transferencia.

65. Por otro lado, es importante precisar que sobre el tiempo de conservación de los datos personales la administrada indica que los datos personales se conservarán en base a la normativa vigente y dentro de dicho párrafo señala la Ley General de Salud, Ley N° 26842, sin embargo, como buena práctica la DPDP recomienda a la administrada indicar la norma técnica que dispone el tiempo de conservación de los datos personales en caso de los centros referidos a la salud.

66. Posteriormente con fecha 18 de octubre de 2019, la administrada presentó descargos señalando que:

    - Los fiscalizadores no han tomado consideración de los carteles que se encuentran distribuidos en las instalaciones de la administrada, por lo

que no se puede suponer que los titulares de datos no tengan conocimiento de los tratamientos de sus datos personales, toda vez que en dichos carteles de informe lo dispuesto en el artículo 18° de LPDP.

- Sobre la indicado por DFI en el informe final referido a que las políticas de privacidad no se menciona el tiempo de conservación, precisando que lo que se indico es ambiguo "(…) *estos serán almacenados según normativa vigente",* la administrada señala que al mencionar el tiempo se ciñe a la normativa NTS N° 139-MINSA/2018/DGAIN — "Norma Técnica de Salud para la Gestión de Historia Clínica", la cual dispone que el plazo máximo de conservar la información es de 20 años, en caso de contabilizar el tiempo que debe ser conservada en archivo activo y pasivo existe la excepción de conserva dicha información por 40 años.

67. Ahora bien, respecto a la forma de materialización del cumplimiento de este deber de informar, la administrada cuenta con el documento denominado Política de Privacidad, ubicado en diferentes lugares, siendo estos lugares visible y de fácil acceso para el público (pacientes y/o representantes legales o apoderados de estos) que se constituyen presencialmente en las instalaciones del establecimiento de salud, por lo que el extremo de los argumentos expuestos por la administrada sobre la forma de materializar dicho cumplimiento quedan estimados.

68. Es decir, en cuanto a la forma de cumplir con las disposiciones del artículo 18° de la LPDP , con la implementación de los carteles se perfeccionaría de forma idónea el cumplimiento de este deber de informar para la situación descrita, en tanto la naturaleza y dinámica propias de la prestación de servicios de salud para supuestos, incluido, aunque no limitado, de emergencias, urgencias, hospitalizaciones, y diagnósticos por imágenes y/o exámenes clínicos que se presten dentro de un mismo establecimiento de salud, por la inmediatez debida de su atención no da opción a las instituciones de salud de implementar una forma distinta de este deber de informar cuando la recopilación de datos personales de los pacientes se realiza presencialmente en sus instalaciones al momento de registrarlos como tales.

69. En conclusión, la administrada debe incluir en el documento denominado "Política de Privacidad" las transferencias nacionales e internacionales, conforme lo dispone el artículo 18° de LPDP.

70. Para finalizar corresponde analizar el tratamiento realizado por la administrada a través de las cámaras de videovigilancia.

71. Al respecto, es importante indicar que en los actos de fiscalización se constató que la administrada cuenta con cámaras de videovigilancia internas y externas, por lo tanto, debe implementar un canal con el que el titular de los datos personales tenga conocimiento de la zona videovigilada.

72. En ese sentido, mediante escrito de fecha 14 de agosto de 2018, la administrada señala que presentó la ubicación de los letreros de las cámaras de videovigilancia interior y exterior, adjuntando fotografías.

73. En ese mismo sentido, con fecha con fecha 23 de setiembre de 2019[46] la administrada presentó descargos alegando que ha implementado el documento Política de Privacidad, adjuntando fotografías.

74. Al respecto, la DFI mediante Informe N° 113-2019-JUS/DGTAIPD-DFI precisó que dicho documento no cumple con informar en su totalidad con lo dispuesto en el artículo 18° de la LPDP, toda vez que no informa el tiempo de conservación.

75. Mediante escrito ingresado el 18 de octubre de 2019, la administrada precisa que los fiscalizadores no han tomado en consideración los carteles distribuidos en distintas áreas de las instalaciones de la administrada. adjunta fotografías del cartel y la impresión de dicho cartel.

76. En ese sentido, dado que el tratamiento de datos personales a través de cámaras de videovigilancia presenta particularidades al momento de cumplir con el deber de informar, y teniendo en cuenta que recién a través de la Directiva N° 01- 2020-JUS/DGTAIPD[47] la Autoridad Nacional de Protección de Datos Personales desarrolló las disposiciones respecto de dicha obligación, por lo que, no se puede exigir dichas disposiciones a la administrada al momento de la fiscalización. Por lo tanto, la DPDP considera que se debe tomar en cuenta que en el momento de la fiscalización y del inicio del procedimiento solo se podía exigir que comunique a los titulares de datos personales que estaban siendo grabados.

77. En ese sentido, de la evaluación de los medios probatorios efectuados, la DPDP determina que la administrada, mediante el escrito de fecha 13 de agosto de 2018 cumple con informar a los titulares de datos personales, respecto de la zona que cuenta con cámaras de videovigilancia.

78. De la revisión al expediente administrativo se tiene que la Resolución Directoral N° 149-2019-JUS/DGTAIPD-DFI, mediante la cual se da inicio a procedimiento administrativo sancionar fue recibida por la administrada el 27 de agosto de 2019.

79. De lo descrito, se evidencia que la administrada presento fotografías que acreditan que la implementación del cartel informativo sobre la zona videovigilada, con fecha anterior a la imputación de cargos, es decir la administrada acreditó cumplir con dicha obligación el 13 de agosto de 2018.

80. Por lo que, corresponde a la DPDP aplicar eximente de responsabilidad conforme a los dispuesto en el en el literal f) del numeral 1 del artículo 257 de la LPAG, sobre el extremo de dicha imputación.

[46] Folios 202 al 262
[47] Aprobada por Resolución Directoral N° 02-2020-JUS/DGTAIPD

81. No obstante, es importarte precisar que la administrada debe implementar el cartel informativo conforme a lo señalado la Directiva, es decir debe modificar el documento denominado "Política de Privacidad" conforme a las recomendaciones expuestas por la DPDP en el punto anterior.

82. Asimismo, es importante precisar que la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Dirección de Protección de Datos Personales a la fecha ha implementado la Directiva N° 01-2020-JUS/DGTAIPD denominada "Tratamiento de datos personales mediante sistemas de videovigilancia", la cual desarrolla un análisis con mayor precisión sobre como los titulares de datos personales pueden informar a los titulares de los datos personales las disposiciones establecidas en el artículo 18° de la LPDP.

83. Respecto a la política de privacidad en los documentos físicos, cabe señalar que estos son llenados luego que el paciente ha pasado por recepción, o ha recibido el documento, por lo tanto son completados una vez que ya vieron la política de privacidad, por lo que el hecho de incorporarlas en cada formulario deviene en una buena práctica, pero no se puede señalar que no están informados.

84. En ese sentido, habría que resaltar que el defecto en el cumplimiento del artículo 18 de la LPDP radica en la no información sobre las transferencias.

85. Por tanto, conforme a los argumentos expuestos la administrada es responsable de realizar tratamiento de datos personales sin informar a los titulares de datos personales lo requerido en el artículo 18° de la LPDP, incurriendo en la infracción grave prevista en el literal a) del numeral 2 del artículo 132° del Reglamento de la LPDP.

Sobre el presunto incumplimiento de las medidas de seguridad

86. Se imputa a la administrada, a través de la Resolución Directoral N° 149-2019-JUS/DGTAIPD-DFI, la infracción grave tipificada en el literal a. del numeral 1 del artículo 132° del RLPDP, al presuntamente no haber implementado las medidas de seguridad para el tratamiento de datos personales, al verificarse que:

    (i) No documentar los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados. Obligación establecida en el numeral 1 del artículo 39º del Reglamento de la LPDP.

    (ii) No generar ni mantener registros de interacción lógica respecto al banco de datos personales en soporte automatizado de pacientes. Obligación establecida en el numeral 2 del artículo 39° del Reglamento de la LPDP.

87. En tal sentido corresponde analizar la normativa vigente y aplicable sobre la materia, los medios probatorios que dejan constancia de los hallazgos encontrados en el procedimiento, y los descargos presentados por la administrada para desvirtuar el hecho imputado.

88. Al respecto, es preciso mencionar que el artículo 9° de la LPDP señala el principio de seguridad como uno de los principios rectores de la protección de datos personales:

> ***"Artículo 9. Principio de seguridad***
> *El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate."*

89. En ese marco, el artículo 16° de la LPDP establece la obligación de adoptar medidas de seguridad para el tratamiento de datos personales:

> ***"Artículo 16. Seguridad del tratamiento de datos personales***
> *Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.*
> *(…)*
> *Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo."*

<u>Sobre el incumplimiento del numeral 1 del artículo 39° del RLPDP</u>

90. Se imputa a la administrada que no habría documentado los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados al personal del sistema, de acuerdo al numeral 1 del artículo 39° del RLPDP.

91. Respecto de las medidas de seguridad a adoptarse en el tratamiento de datos personales en soporte automatizado, el RLPDP señala lo siguiente:

> *"**Artículo 39.- Seguridad para el tratamiento de la información digital.***
> *Los sistemas informáticos que manejen bancos de datos personales deberán incluir en su funcionamiento:*
>
> *1. El control de acceso a la información de datos personales incluyendo la gestión de accesos desde el registro de un usuario, la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, entre los que se encuentran usuario, contraseña, uso de certificados digitales, tokens, entre otros, y realizar una verificación periódica de los privilegios asignados, los cuales deben estar definidos mediante un procedimiento documentado a fin de garantizar su idoneidad."*

92. De lo anterior se desprende que es obligatorio definir procedimientos documentados de gestión de accesos y gestión de privilegios de los usuarios para

el acceso al sistema, la identificación de usuarios en el sistema, así como el proceso de verificación periódica de dichos privilegios, esto es, se debe establecer el procedimiento para el alta, baja y modificación de datos, modificación de usuarios, así como sus privilegios en el sistema.

93. En el Acta de Fiscalización N° 01-2018[48] en la cual se deja constancia de la fiscalización del 26 de julio de 2018, se indica lo siguiente:

> *"(…) 7.- Se verificó que no cuentan con los procedimientos documentados de la gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados. (…)."*

94. Con fecha posterior, se emitió el Informe de Fiscalización N° 176-2018-JUS/DGTAIPD-DFI-PCFC[49], que recoge las conclusiones sobre la fiscalización realizada, indicando lo siguiente:

> *"**VII. CONCLUSIONES:***
> *(…)*
> ***Quinta.- CENTRO MEDICO CLINICASAN JUDAS TADEO.** No contaría con las medidas de seguridad requeridas por el artículo 39° (numeral 1 y 2) del RLPDP. Hecho que constituiría una presunta infracción según lo regulado en el literal a. del numeral 1 del artículo 132° del Reglamento de la LPDP: "Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia", dicha infracción es **leve** conforme al citado artículo.*
> *(…)."*

95. De lo citado, se colige que la administrada no había implementado las medidas de seguridad establecidas en el numeral 1 del artículo 39° del RLPDP, consistentes en no documentar los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados, lo que motivó su inclusión en uno de los supuestos infractores imputados en la Resolución Directoral N° 149-2019-JUS/DGTAIPD-DFI.

96. Luego, con el escrito de descargos presentado mediante hoja de tramite N° 40222-2019[50] de fecha 06 de junio de 2019, la administrada argumenta haber cumplido con adjuntar los procedimientos documentados de la gestión de accesos, gestión de privilegios y verificación periódica, los mismos que certifican la seguridad para el tratamiento de los datos personales.

97. Mediante Informe Técnico N° 143-2019-DFI-ETG[51] de 06 de agosto de 2019, el analista de Fiscalización en Seguridad de la Información emitió informe señalando lo siguiente:

> *"(…)*
> *V. Conclusiones*
> *(…)*

[48] Folio 08 a 12
[49] Folio 145 a 153
[50] Folios 158 a 177
[51] Folio 179

4. *CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A. no documenta los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados incumpliendo con el numeral 1 del artículo 39° del Reglamento de la LPDP.*

(…)"

98. Mediante escrito de fecha 23 de setiembre de 2019[52], la administrada presentó descargos alegando los responsables que autorizan el ingreso de los usuarios al sistema son los firmantes del documentos de procedimientos de gestión de acceso, privilegios y verificación, vale decir gerencia general, gerencia de operaciones y jefatura de sistemas.

99. Mediante Informe Técnico N° 189-2019-DFI-ETG[53] de 25 de setiembre de 2019, el analista de Fiscalización en Seguridad de la Información emitió informe señalando lo siguiente:

"(…)
V. Conclusiones
(…)
5. *CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A. no documenta los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados incumpliendo con el numeral 1 del artículo 39° del Reglamento de la LPDP.*

(…)"

100. Posteriormente con fecha 18 de octubre de 2019[54], la administrada presentó descargos indicando haber cumplido con la presentación de todos los documentos de los procedimientos debidamente documentados sobre la gestión de accesos, privilegios y verificación de los mismos, asimismo la administrada manifestó que la DFI requiere que se especifique paso a paso a fin de que puedan comprender los procedimientos que se siguen, no obstante dicho requerimiento no se encuentra tipificado.

101. Mediante Informe Técnico N° 376-2020-DFI-ORQR55 de 11 de noviembre de 2020, el analista de Fiscalización en Seguridad de la Información emitió informe señalando lo siguiente:

"(…)
2. *Al respecto, luego de verificar y analizar la información remitida por la administrada, se puede determinar que ha evidenciado contar con procedimientos documentados referentes a la gestión de accesos ya que en la información remitida contempla y/o establece la asignación de cuentas de usuario y contraseñas de acceso a los operadores del sistema "SJT", a través del cual se realiza el tratamiento del banco de datos personales de pacientes. Por lo que estaría cumpliendo con el numeral 1 del artículo 39° del Reglamento de la LPDP*

(…)

[52] Folios 202 al 262
[53] Folio 264
[54] Folios 279 al 333
[55] Folio 349 al 350

> *4. Al respecto, luego de verificar y analizar la información remitida por la administrada, se puede determinar que ha evidenciado contar con procedimientos documentados referentes a la gestión de privilegios ya que ha provisto información respecto a los perfiles de acceso o niveles de usuario con los que cuenta el sistema "SJT", a través del cual realiza el tratamiento automatizado del banco de datos personales de pacientes. Asimismo, describe los permisos y/o restricciones de acceso a la información de los pacientes en relación a los niveles de usuario. Por lo que estaría cumpliendo con el numeral 1 del artículo 39° del Reglamento de la LPDP.*
> *(…)*
> *5. Al respecto, luego de verificar y analizar la información remitida, se puede determinar que la administrada hace referencia a un procedimiento de Alta y Baja de usuarios, verificando que no proporciona información que evidencie la realización de una verificación periódica a los privilegios otorgados a los usuarios del sistema a través del cual realiza el tratamiento de datos personales de pacientes. Asimismo, no se proporciona un medio probatorio que establezca y/o demuestre una frecuencia respecto a la periodicidad del referido procedimiento. Por lo que estaría incumpliendo con el numeral 1 del artículo 39° del Reglamento de la LPDP.*

102. Al respecto, corresponde precisar que los medios probatorios presentada por la administrada sobre los procedimientos documentados de la gestión de accesos analizados en el informe técnico señalado obran en (folios 320 y 321) de dicho procedimiento administrativo sancionador, no obstante la DPDP constató que dichos medios de prueba analizados por el Analista de Fiscalización en Seguridad de la Información, la administrada los presentó con el escrito de 18 de enero de 2019, para ser más específicos se encuentran en (folios 167 al 170).

103. Conforme, lo precisado en el Informe Técnico N° 376-2020-DFI-ORQR, la administrada acredita cumplir las medidas de seguridad respecto de los procedimientos documentados de la gestión de accesos.

104. En ese sentido, la DPDP advierte que los medios de prueba que acreditan la implementación de los procedimientos documentados de la gestión de accesos en el sistema SJT, fueron ofrecidos por la administrada en el escrito de fecha 18 de enero de 2019, y la Resolución Directoral N° 149-2019-JUS/DGTAIPD-DFI, mediante la cual se da inicio a procedimiento administrativo sancionar fue recibida por la administrada el 27 de agosto de 2019, es decir con la administrada cumplió con implementar la presunta imputación con anterioridad al inicio del presente procedimiento, por lo que corresponde aplicar eximente de responsabilidad sobre el extremo de la imputación.

105. Asimismo corresponde a la DPDP estimar los argumentos de la administrada expuestos en el escrito de fecha 18 de octubre de 2019, en cuanto al extremo de la respectiva imputación referida a la implementación de los procedimientos documentados de la gestión de accesos de usuarios al sistema SJT.

106. De la obligación de contar con procedimiento documentados sobres gestión de privilegios, la documentación presentada por administrada en (folios 324 al 328), se analizó en el Informe Técnico N° 376-2020-DFI-ORQR, el mismo que señala que la administrada cumple con las medias de seguridad sobre los procedimientos

documentados de la gestión de privilegios conforme a los dispuesto en el numeral 1 del artículo 39 del Reglamento de la LPDP.

107. En ese sentido, de la revisión a los medios probatorios ofrecidos por la administrada la DPDP constató los mismo medios de prueba analizados en el informe Técnico N° 376-2020-DFI-ORQR, obra en el expediente administrativo en (folios 171 al 174), por lo que se evidencia que la administrada cumplió con acreditar tal imputación con anterioridad a la imputación de cargos.

108. En consecuencia, la DPPD considera eximir de responsabilidad a la administrada, sobre el extremo de la imputación, referida a contar con procedimientos documentados de la gestión de privilegios.

109. Con relación, a la obligación de documentar los procedimientos de verificación periódica de privilegios asignados, conforme a lo indicado en el Informe Técnico N° 376-2020-DFI-ORQR, mediante el cual se analizó la documentación presentada por la administrada con fecha 18 de octubre de 2019, determinando que la administrada no evidencian que realice una verificación periódica de los usuarios en el sistema, asimismo no indica frecuencia de la periodicidad de dicho procedimiento.

110. La DPDP, procedió a revisión de los medios probatorios presentados durante el procedimiento, constatándose que la administrada no presentó medios probatorios que acrediten las medias de seguridad referidas a documentar los procedimientos de verificación periódica de privilegios y la frecuencia de periodicidad de tal procedimiento.

111. Entonces, se tiene que la administrada no documentaba la verificación periódica de privilegios asignados, por lo que incumpliendo el numeral 1 del artículo 39° del Reglamento de la LPDP

Sobre el incumplimiento del numeral 2 del artículo 39° del RLPDP

112. Se imputa a la administrada que no habría generado y mantenido registros de interacción lógica respecto del banco de datos personales en soporte automatizado de pacientes, de acuerdo al numeral 2 del artículo 39° del Reglamento de la LPDP.

113. Respecto de las medidas de seguridad a adoptarse en el tratamiento de datos personales en soporte automatizado, el RLPDP señala lo siguiente:

> *"**Artículo 39.- Seguridad para el tratamiento de la información digital.***
> *Los sistemas informáticos que manejen bancos de datos personales deberán incluir en su funcionamiento:*
>
> *2. Generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y*

acciones relevantes. Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, entre los que se encuentran el destino de los registros, una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros."

114. De lo anterior se desprende que es obligatorio contar con control de acceso que incluya la gestión de accesos desde el registro del usuario, gestión de privilegios e identificación del usuario en el sistema, asimismo debe generar y mantener registros que provean evidencia sobre las interacciones con el sistema, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones relevantes.

115. Ahora bien, del Acta de Fiscalización N° 01-201856 en la cual se deja constancia de la supervisión del 26 de junio de 2018, se indica lo siguiente:

> *"(…) 8.- Se verificó que no genera ni mantiene registros de interacción lógica referidos al banco de datos personales de pacientes (…)."*

116. Al respecto, la administrada con fecha 13 de agosto de 2018[57] alega haber presentado documentación sobre los registros de interacción lógica del banco de datos de pacientes.

117. Mediante Informe Técnico N° 205-2018-DFI-ETG[58] de 11 de setiembre de 2018, se informó sobre las medidas de seguridad implementadas por la administrada indicando lo siguiente:

> *"(…)*
> *V. Conclusiones*
> *(…)*
> 6. *CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A. no genera ni mantiene registros de interacción lógica respecto al banco de datos personales en soporte automatizado de pacientes, incumpliendo con el numeral 2 del artículo 39° del Reglamento de la LPDP.*
> *(…)"*

118. Posteriormente, se emitió el Informe de Fiscalización N° 176-2018-JUS/DGTAIPD-DFI-PCFC[59], que recoge las conclusiones sobre la fiscalización realizada, indicando lo siguiente:

> *"(…)*
> *VI. CONCLUSIONES*
> *(…)*
> ***Quinta.- CENTRO MEDICO CLINICASAN JUDAS TADEO.*** *No contaría con las medidas de seguridad requeridas por el artículo 39° (numeral 1 y 2) del RLPDP. Hecho que constituiría una presunta infracción según lo regulado en el literal a. del numeral 1 del*

[56] Folio 11 a 24
[57] Folios 124 al 128
[58] Folio 136 a 141
[59] Folio 145 a 153

*artículo 132° del Reglamento de la LPDP: "Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia", dicha infracción es **leve** conforme al citado artículo.*
(…)."

119. La administrada, con fecha 06 de junio de 2019[60] presentó descargos alegando contar con los procedimientos documentados sobre la verificación periódica.

120. En ese sentido, DFI emite el Informe Técnico N° 143-2019-DFI-ETG61 de 06 de agosto de 2019, a través, del cual se analizan los medios de prueba presentados por la administrada indicando lo siguiente:

"(…)
III. Conclusiones

2. CENTRO MEDICO CLINICA SAN JUDAS TADEO, no genera y mantiene registros de interacción lógica respecto al banco de datos personales en soporte automatizado de pacientes; incumpliendo con el numeral 2 del artículo 39° del Reglamento de la LPDP.
(…)"

121. De los documentos citados se colige que la administrada no había implementado las medidas de seguridad establecidas en el numeral 2 del artículo 39° del RLPDP, consistentes en generar y mantener registros de interacción lógica con el banco de datos personales de pacientes, lo que motivo su inclusión en uno de los supuestos infractores imputados en la Resolución Directoral N° 149-2018-JUS/DGTAIPD-DFI.

122. Posteriormente, en los descargos presentados por la administrada el 23 de setiembre de 2019[62], manifiesta que con escrito de fecha 13 agosto de 2019 remitió los registros de interacción lógica en los que se puede apreciar fecha de tratamiento código de usuario y fecha de actualización, es decir se encuentra la evidencia de la interacción lógica.

123. En efecto, mediante Informe Técnico N° 189-2020-DFI-ETG[63] de 20 de setiembre de 2019, a través, la DFI señala lo siguiente:

"(…)
III. Conclusiones
(…)
2. CENTRO MEDICO CLINICA SAN JUDAS TADEO, no genera y mantiene registros de interacción lógica respecto al banco de datos personales en soporte automatizado de pacientes; incumpliendo con el numeral 2 del artículo 39° del Reglamento de la LPDP."

[60] Folios 124 al 177
[61] Folio 179 a 180
[62] Folios 202 al 262
[63] Folio 264

124. Con fecha 18 de octubre de 2019 la administrada señala que los registros de interacción lógica que proveen evidencias han sido implementadas con los medios de prueba presentados en su oportunidad.

125. En ese sentido, la DPDP solicitó el Informe Técnico N° 376-2020-DFI-ORQR[64] que señala lo siguiente

> *"(…)*
> *8. respecto, luego de revisar y analizar la documentación remitida, se puede verificar que la administrada únicamente realiza una descripción y/o referencia en relación a los registros de interacción lógica. Sin embargo, no adjunta información que evidencie de manera específica que el sistema "SJT", a través del cual realizan tratamiento del banco de datos personales automatizado de pacientes genera registros de interacción lógica correspondientes al inicio de sesión, cierre de sesión y acciones relevantes como puede ser la actualización y/o eliminación de la información (según aplique). Cabe precisar que para evidenciar la generación de los referidos registros, la administrada puede adjuntar videos en los cuales se pueda constatar la actividad de la cuenta de usuario y la generación de sus registros de interacción correspondientes. Por lo que estaría incumpliendo con lo dispuesto en el numeral 2 del artículo 39° del Reglamento de la LPDP.*
> *(…)"*

126. Al respecto, conforme al análisis efectuado por el especialista se concluye que la administrada no presentó medios de prueba que demuestre la implementación de las medidas de seguridad referidas a generar y mantener registros de interacción lógica, incluyendo la información de las cuentas de usuario con acceso al sistema del inicio, cierre de cesión y acciones relevantes, por lo que incumple con lo dispuesto en el numeral 2 del artículo 39° del Reglamento de la LPDP

Sobre la determinación de la sanción a aplicar

127. La Tercera Disposición Complementaria Modificatoria del Reglamento del Decreto Legislativo N° 1353, modificó el artículo 38 de la LPDP que tipificaba las infracciones a la LPDP y su reglamento, incorporando el artículo 132 al Título VI sobre Infracciones y Sanciones de dicho reglamento, que en adelante tipifica las infracciones.

128. Por su parte, el artículo 39 de la LPDP establece las sanciones administrativas calificándolas como leves, graves o muy graves y su imposición va desde una multa de cero coma cinco (0,5) unidades impositivas tributarias hasta una multa de cien (100) unidades impositivas tributarias65, sin perjuicio de las medidas

[64] Folios 349 al 351

[65] **Ley N° 29733, Ley de Protección de Datos Personales**
"**Artículo 39. Sanciones administrativas**
En caso de violación de las normas de esta Ley o de su reglamento, la Autoridad Nacional de Protección de Datos Personales puede aplicar las siguientes multas:
1. Las infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).
2. Las infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT).

correctivas que puedan determinarse de acuerdo con el artículo 118 del Reglamento de la LPDP66.

129. En el presente caso, se ha establecido la responsabilidad de la administrada por lo siguiente:

- Realizar tratamiento de datos personales sin informar a los titulares de datos personales, al no informar a los pacientes sobre las transferencias, lo requerido en el artículo 18° de la LPDP; lo que configuraría una infracción grave tipificada en el literal a, numeral 2 del artículo 132° del Reglamento de la LPDP: *"No atender impedir u obstaculizar el ejercicio de los derechos del titular de datos personales reconocidos en el título III de la Ley N° 29733 y su Reglamento".*

- No haber implementado las medidas de seguridad para el tratamiento de datos personales al: (i) No documentar los procedimientos de verificación periódica de privilegios asignados. Obligación establecida en el numeral 1 del artículo 39° del Reglamento de la LPDP. (i) No generar ni mantener registros de interacción lógica respecto al banco de datos personales en soporte automatizado de pacientes. Obligación establecida en el numeral 2 del artículo 39° del Reglamento de la LPDP. Lo que configuraría la infracción leve tipificada en el literal a), numeral 1, del artículo 132° del Reglamento de la LPDP: *"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normatividad sobre la materia."*

130. Por su parte, esta dirección determina el monto de la multa a imponer tomando en cuenta para su graduación los criterios establecidos en el numeral 3 del artículo 248 de la LPAG. En tal sentido, debe prever que la comisión de tal conducta no resulte más ventajosa para el infractor que cumplir las normas infringidas o asumir la sanción administrativa, por lo que la sanción debe ser proporcional al incumplimiento calificado como infracción, observando para ello los criterios mencionados.

131. En el presente caso, se considera como criterios relevantes para graduar las sanciones, los siguientes:

a) <u>El beneficio ilícito resultante por la comisión de la infracción:</u>

No se ha evidenciado beneficio ilícito alguno resultante de la comisión de las infracciones a sancionar.

---

3. Las infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT)."

[66] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 003-2013-JUS "Artículo 118.- Medidas cautelares y correctivas**.
Una vez iniciado el procedimiento sancionador, la Dirección de Sanciones podrá disponer, mediante acto motivado, la adopción de medidas de carácter provisional que aseguren la eficacia de la resolución final que pudiera recaer en el referido procedimiento, con observancia de las normas aplicables de la Ley Nº 27444, Ley del Procedimiento Administrativo General.
Asimismo, sin perjuicio de la sanción administrativa que corresponda por una infracción a las disposiciones contenidas en la Ley y el presente reglamento, se podrán dictar, cuando sea posible, medidas correctivas destinadas a eliminar, evitar o detener los efectos de las infracciones."

b) La probabilidad de detección de la infracción:

El caso del incumplimiento del artículo 18º se aprecia que el incumplimiento se configura a través de los carteles publicados en diversos espacios de la clínica, por lo que el acceso se restringe a los visitantes de la misma, circunstancias que hacen que la probabilidad de detección de esta infracción sea media.

En lo concerniente a la inaplicación de las medidas de seguridad objeto de sanción, debe tenerse en cuenta que su detección tuvo lugar en la visita de fiscalización realizada a la entidad, por lo que su probabilidad de detección es baja.

c) La gravedad del daño al interés público y/o bien jurídico protegido:

Las infracciones detectadas afectan el derecho fundamental a la protección de datos personales, el cual se encuentra reconocido en el artículo 2, numeral 6, de la Constitución Política del Perú, siendo desarrollado por la LPDP y su reglamento.

Respecto del incumplimiento del artículo 18° de la LPDP, debe señalarse que implica la vulneración del derecho de los titulares de los datos personales a ser informados sobre el tratamiento que efectuará el responsable, al no brindarse de forma completa la información requerida por dicho artículo. Tal situación, significa el impedimento de un derecho del titular de los datos personales, perenne en cualquier circunstancia, el de ser informado sobre los pormenores del tratamiento a efectuar sobre sus datos personales, el cual repercute en el impedimento de ejercicio de otros derechos.

De otro lado, sobre la no aplicación de medidas de seguridad al tratamiento de los datos personales del banco de datos automatizado, implica que efectúa un tratamiento que en el que no se tuvo el resguardo y seguridad de la información de los pacientes en algún momento el suficiente control sobre las personas que lo realizan, lo que incrementa el riesgo de afectación a la confidencialidad e integridad de los datos, así como tampoco se tuvo las providencias necesarias ante cualquier evento que deteriore o destruya el soporte utilizado para el tratamiento de datos personales.

d) El perjuicio económico causado:

No se evidencia un perjuicio económico resultante de la comisión de las infracciones a sancionar.

e) La reincidencia en la comisión de la infracción a sancionar:

La administrada no es reincidente en el caso de las infracciones a sancionar.

f) Las circunstancias de la comisión de las infracciones:

La adecuación de la administrada, en relación al incumplimiento del artículo 18° de la LPDP no es onerosa ni compleja; en circunstancias regulares se debería atender lo dispuesto en la norma sin complicaciones.

Por otro lado, sobre las medias de seguridad, podría ser onerosa, toda vez que requiere de personal especializado en la materia, no obstante, la administrada podría cumplir con la normativa sin ninguna complicación

g) La existencia o no de intencionalidad en la conducta del infractor:

En el caso de las infracciones, se evidenció acciones de la administrada tendientes a corregir su conducta logrando levantar algunas de las observaciones incluso antes del inicio del procedimiento sancionador.

132. Es pertinente indicar que para imponer la sanción se tendrá en cuenta la suma de todos los criterios que permiten graduar la sanción conforme a los argumentos desarrollados en el considerando **(132)** de la presente resolución directoral.

Por las consideraciones expuestas y de conformidad con lo dispuesto por la LPDP y su reglamento, la LPAG, y el Reglamento del Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses aprobado por Decreto Supremo N° 019-2017-JUS;

SE RESUELVE:

Artículo 1.- Eximir a **CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A.**, de la responsabilidad administrativa en el extremo de la imputación de realizar tratamiento a través de las cámaras de videovigilancia, por la presunta infracción grave contemplada en el literal a) del inciso 2 del artículo 132 del Reglamento de la LPDP: "*No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo a lo establecido en el Título III de la Ley Nº 29733 y su Reglamento*"..

Artículo 2.- Sancionar a **CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A.** con la multa ascendente a cinco coma cero una unidad impositivas tributarias (5, 01 UIT), por haber realizado tratamiento de datos personales sin informar a los titulares de datos personales lo requerido en el

artículo 18° de la LPDP; al no informar sobre las transferencias, lo que configuraría una infracción grave tipificada en el literal a, numeral 2 del artículo 132° del Reglamento de la LPDP: *"No atender impedir u obstaculizar el ejercicio de los derechos del titular de datos personales reconocidos en el título III de la Ley N° 29733 y su Reglamento."*

Artículo 3.- Sancionar a **CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A.** Con la multa ascendente uno coma cinco unidad impositiva tributaria (1,5 UIT) por no haber implementado las medidas de seguridad para el tratamiento de datos personales, al: (i). No documentar los procedimientos de verificación periódica de privilegios asignados. Obligación establecida en el numeral 1 del artículo 39 del Reglamento de la LPDP; (ii) No generar ni mantener registros de interacción lógica respecto al banco de datos personales en soporte automatizado de pacientes. Obligación establecida en el numeral 2 del artículo 39° del Reglamento de la LPDP; lo que configuraría la infracción leve tipificada en el literal a), numeral 1, del artículo 132° del Reglamento de la LPDP: *"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la norma sobre la materia."*

Artículo 4.- Eximir a **CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A.** de la responsabilidad administrativa en el extremo de la imputación por no haber implementado las medidas de seguridad para el tratamiento de datos personales, al: (i). No documentar los procedimientos de gestión de accesos, gestión de privilegios. Obligación establecida en el numeral 1 del artículo 39 del Reglamento de la LPDP, lo que configuraría la infracción leve tipificada en el literal a), numeral 1, del artículo 132° del Reglamento de la LPDP: *"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la norma sobre la materia."*

Artículo 5.- Imponer como medidas correctivas a **CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A.** lo siguiente:

- Implementar o modificar el documento denominado "Política de Privacidad" conforme a las disposiciones establecidas en el artículo 18° de la LPDP, es decir incluir las transferencias nacionales e internacionales.

- Documentar los procedimientos de verificación periodica de privilegios asignados, conforme a lo dispuesto en el numeral 1 del artículo 39º del Reglamento de la LPDP

- Generar y mantener registros de interacción lógica respecto al banco de datos personales en soporte automatizado de pacientes, conforme a lo dispuesto en el numeral 2 del artículo 39° del Reglamento de la LPDP

Para el cumplimiento de las medidas correctivas, se otorga el plazo de treinta (30) días hábiles contados a partir de la notificación que declare consentida o firme la presente resolución directoral.

Artículo 5.- Informar a **CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A.** que el incumplimiento de las medidas correctivas constituye la comisión de la infracción tipificada como muy grave en el literal d) del numeral 3 del artículo 132 del Reglamento de la LPDP[67].

Artículo 6.- Informar a **CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A.** que, contra la presente resolución, de acuerdo con lo indicado en el artículo 218 de la LPAG, proceden los recursos de reconsideración o apelación dentro de los quince (15) días hábiles posteriores a su notificación[68].

Artículo 7.- Informar a **CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A.**, que deberá realizar el pago de la multa en el plazo de veinticinco (25) días útiles desde el día siguiente de notificada la presente resolución.

Artículo 8.- En caso presente recurso impugnatorio, el plazo para pagar la multa es de diez (10) días hábiles de notificada la resolución que agota la vía administrativa, plazo que se contará desde el día siguiente de notificada dicha resolución que pone fin la vía administrativa.

Artículo 9.- Se entenderá que cumplió con pagar la multa impuesta, si antes de que venzan los plazos mencionados, cancela el sesenta por ciento (60%) de la multa impuesta conforme a lo dispuesto en el artículo 128 del Reglamento de la LPDP[69]. Para el pago de la multa deberá considerar el valor de la UIT del año 2019.

---

[67] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 003-2013-JUS**
"TÍTULO VI INFRACCIONES Y SANCIONES
CAPÍTULO IV
INFRACCIONES
Artículo 132.- Infracciones
Las infracciones a la Ley Nº 29733, Ley de Protección de Datos Personales, o su Reglamento se califican como leves, graves y muy graves y se sancionan con multa de acuerdo al artículo 39 de la citada Ley.
(…)
3.Son infracciones muy graves:
(…)
d) No cesar en el indebido tratamiento de datos personales cuando existiese un previo requerimiento de la Autoridad como resultado de un procedimiento sancionador o de un procedimiento trilateral de tutela."

[68] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS**
"**Artículo 218. Recursos administrativos**
218.1 Los recursos administrativos son:
a) Recurso de reconsideración
b) Recurso de apelación
Solo en caso que por ley o decreto legislativo se establezca expresamente, cabe la interposición del recurso administrativo de revisión.
218.2 El término para la interposición de los recursos es de quince (15) días perentorios, y deberán resolverse en el plazo de treinta (30) días."

[69] **Artículo 128.- Incentivos para el pago de la sanción de multa.**
Se considerará que el sancionado ha cumplido con pagar la sanción de multa si, antes de vencer el plazo otorgado para pagar la multa, deposita en la cuenta bancaria determinada por la Dirección General de Protección de Datos Personales el sesenta por ciento (60%) de su monto. Para que surta efecto dicho beneficio deberá comunicar tal hecho

Artículo 10.- Notificar a **CENTRO MEDICO CLINICA SAN JUDAS TADEO S.A.**, la presente resolución.

Regístrese y comuníquese.

Firmado digitalmente por GONZALEZ LUNA Maria Alejandra FAU 20131371617 soft
Fecha: 2020.11.14 10:38:00 -05'00'

María Alejandra González Luna
Directora (e) de Protección de Datos Personales

MAGL/fva

a la Dirección General de Protección de Datos Personales, adjuntando el comprobante del depósito bancario correspondiente. Luego de dicho plazo, el pago sólo será admitido por el íntegro de la multa impuesta.